REMARKS

The Office Action dated December 14, 2007 has been received and carefully reviewed. The preceding amendments and the following remarks form a full and complete response thereto. Claims 1, 2, 39 and 42 have been amended. No new matter has been added by the amendments. With the foregoing amendment claims 1-7, 14-20 and 25-44 (claims 1-3 are independent) are pending in the application and submitted for reconsideration.

An objection was made to claim 1 because of informalities. Claim 1 has been amended to correct the references to the term "the computer system." Accordingly, the Applicant requests that the objection be withdrawn.

Claims 1, 2, 39 and 42 were rejected under 35 U.S.C. § 112, para. 2, as being allegedly indefinite for failing to point out and distinctly claim the subject matter which the applicant regards as the invention. Claims 1, 2, 39 and 42 have been amended to correct the usage of the term "about." Thus, Applicant submits that claims 1, 2, 39 and 42 comply with the requirements of 35 U.S.C. § 112 and requests that the rejection be withdrawn.

Claims 1, 2, 39-40 and 42-43 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over U.S. Pat. 7,152,242 to Douglas and in view of U.S. Pat. 6,640,242 to O'Neal. Claims 15 and 16 were rejected under 35 U.S.C. § 103(a) as being allegedly as obvious over Douglas and further in view of O'Neal, Terry and Berg. Claims 25-26, 41 and 44 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Douglas and further in view of O'Neal and Berg et al. (U.S. Patent Pub. No. US 2001/0044904). Claims 6-7 and 19-20 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious

over Douglas and further in view of O'Neal and Terry (U.S. Patent Pub. No. US 2002/0026505). Claims 4-5 and 17-18 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Douglas and further in view of O'Neal and Williams et al. (U.S. Patent No. 5,911,065).

Applicant respectfully traverses each of the rejections and submits that none of the cited prior art, taken alone or in combination with other art, discloses or suggests each and every feature of the claims.

What a prior art reference teaches one of ordinary skill in the art is a question of fact. *In Re John R. Beatie*, 974 F.2d 1309, 1313 (Fed. Cir. 1992). Applicants submit herewith the Declaration of Victor J. Yodaiken (the "Yodaiken Decl.") providing relevant fact evidence relating to how one skilled in the art would view the teachings of the cited prior art and explaining that one skilled in the art would consider the cited prior art references as failing to disclose salient features of the claims, including, but not limited to, the hard real-time features of the claimed invention. In particular, the principal references cited in the Office Action disclose common "real-time" systems only and fail to disclose the claimed "hard real-time" systems, which is a very important distinction. See Yodaiken Decl. at ¶. 4 et seq.

The declarant, Mr. Yodaiken, has over 26 years of experience in the systems software industry, and has spent the last 26 years working in the area of hard real-time operating systems. Yodaiken Decl., ¶ 2. Further, Mr. Yodaiken is the inventor of the invention embodied in the present application and is well known as a pioneer in the area of hard-real-time operating systems as the inventor of *RTLinux* (Real-Time Linux). Yodaiken Decl. ¶ 2. Accordingly, it cannot be disputed that Mr. Yodaiken is at least

representative of one skilled in the art in the field to which the claimed subject matter is directed, if not an expert in the art. Yodaiken Decl. ¶¶ 1-3.

Each of the claims of the present application relates to software security systems and methods that include features relating to the application of hard real-time operating systems or the performance of software security steps in hard real-time. For example, claim 1, upon which claims 4-7, 14-16 and 39-41 depend, recites a system comprising a deterministic network and computer running a hard real-time operating system which is connected to the deterministic network.

Claim 2, upon which claims 17-20, 25, 26 and 42-44 depend, recites a computer system executing a security process under a real-time operating system wherein the security process is configured to periodically, in hard real-time, check the integrity of an application and/or data element used by the application. Claim 2 further recites an external monitor which sends a challenge to the security process or to a challenge handler that monitors the integrity of the security process via a deterministic network.

The term "hard real-time" as used throughout the claims relates to the performance of tasks within a very small, specified, fixed period of time (e.g., 1 millisecond). Yodaiken Decl. ¶ 7. This is quite a different concept than what is commonly meant by the term "real time" as used in the cited prior art references. Namely, the term "real time" is generally used to mean that actions occur quickly, but latency can be tolerated.

As used in Douglas, "real-time" refers to a process or application that is "on-line" or "continuously updating," which is different than hard real-time processes as used in the claims, which must be executed within a specified, fixed period of time. Moreover, Douglas fails to use the term "hard real-time" even once. One skilled in the art viewing

Douglas as a whole would understand that Douglas does not contemplate concepts of hard real-time, including deadlines, deterministic execution, operating systems that can guarantee timing (i.e., hard real-time systems), or any of the associated technologies or methods of hard real-time systems. Yodaiken Decl. ¶¶ 12-24. Because Douglas does not perform actions in hard real-time, unlike the claimed invention, Douglas cannot prevent dire consequences that can result from latency. See, e.g., present application at ¶ 35.

The Office Action includes several errors that should be noted. For example, With respect to claim 2, the Office Action states:

> [a]s to claim 2, Douglas discloses in a computer system running a real-time operating system.

(December 14, 2007 Office Action at p. 5). Douglas makes no mention of a real-time operating system and, more particularly, Douglas never refers to a "hard real-time operating system" that can assure timing of an application. In fact, Douglas specifically only refers to Linux and MS Windows, neither of which are hard real-time in their usual form. Yodaiken Decl. ¶ 19.

With respect to claim 27 the Office Action states:

> Douglas discloses wherein the first real-time thread is further configured to check a set of integrity markers of the non-real-time kernel (column 2, lines 45-50).

(December 14, 2007 Office Action at p. 9). However, column 2, lines 45-50 of Douglas have no reference to threads, to real-time, or to one kernel checking another kernel. Instead, Douglas in Col 9, lines 45-50 refers to an application reading logs produced by the operating system hosting the application. Yodaiken Decl. ¶ 20.

The Office Action includes the same error again in rejecting claim 31:

> Douglas discloses wherein the second real-time thread is further configured to check a set of integrity markers of the real-time kernel.

(December 14, 2007 Office Action at p. 9). As described above, Douglas makes no reference to any threads at all. Yodaiken Decl. ¶ 21.

The novel aspects of the present invention rest in the application of "hard real-time" techniques to intrusion detection and prevention. All the claims of the application depend on the ability of the hard real-time operating system to guarantee that software will meet stringent timing constraints. Douglas in no way discloses, suggests, or even comes close to teaching such techniques. The Office Action states that Douglas discloses:

> an external monitor connected to the network (col 2, lines 30-50), wherein the security process is configured to periodically, in hard real-time, check the integrity of the application and/or a data element used by the application.

(Col. 9, Lines 3-15). Douglas instead discloses a continuous update of the integrity checks – no hard real-time at all. The novelty of the present invention is precisely in this difference. On-line integrity checks are well established much before Douglas. As is disclosed in the application for the present invention, the utility of a hard real-time integrity check is that attackers are faced with the burden of completing an attack before a deadline expires. Yodaiken Decl. ¶ 22.

Thus, for at least the several foregoing reasons, Applicants submit that Douglas fails to disclose or suggest the hard real-time features, as claimed in any of the pending claims.

None of the prior art remedies the above-described deficiencies of Douglas.

The Office Action cites to O'Neal as showing the feature of a "deterministic network" for claims 1 and 2. As the Examiner correctly notes, the term "deterministic network" as claimed, would be understood to mean a network in which responses are received in a specified, fixed period of time. However, the term "deterministic" is not found anywhere in O'Neal and O'Neal does not disclose any network that might be characterized as deterministic as used in the context of hard real-time systems. Yodaiken Decl. ¶¶ 26-29. The system described in O'Neal does not offer any timing guarantees that would be required for it be classified as deterministic. Yodaiken Decl. ¶¶ 26-29. The fact that the invention in O'Neal checks for a response time-out period is not analogous to a deterministic network as used in claims 1 and 2. Yodaiken Decl. ¶¶ 26-29. A time out period for the network protocols disclosed in O'Neal would be on the order of many seconds, not a few milliseconds as required by claims 1 and 2. Yodaiken Decl. ¶ 28. Simply put, one skilled in the art would not consider the system disclosed by the cited prior art to be a deterministic network, and none of the prior art references disclose a deterministic network, as claimed in claims 1-2. Yodaiken Decl. ¶¶ 26-29.

The other references cited by the Examiner, fail to cure the above-described deficiencies of Douglas and O'Neal. While the prior art has been discussed with respect to independent claims 1-3, claims 4-7, 14-20 and 25-44 all depend from these claims and would therefore be patentable over the art of record, for at least the reasons set forth above.

Thus, Applicants submit that the combination of cited prior art fails to disclose or suggest each and every feature of claims 1, 2, 4-7, 15-20, 25-26, and 39-44. Accordingly,

the Applicant requests that the rejection to claims 1, 2, 4-7, 15-20, 25-26, and 39-44 be withdrawn and claims 1, 2, 4-7, 15-20, 25-26, and 39-44 be allowed.

Claims 3, 27 and 31 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over REDSonic, Inc., http://www.redsonic.com/en/products/RealTime.htm; Copyright 2002, pp1-4, ("REDSonic") and further in view of Douglas. Claims 28-30 were rejected as allegedly obvious under 35 U.S.C. § 103(a) over REDSonic and further in view of Douglas and Berg. Claims 32-35 and 37-38 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over REDSonic and further in view of Douglas and O'Neal. Claim 36 was rejected under 35 U.S.C. § 103(a) as being allegedly obvious over REDSonic and further in view of Douglas, O'Neal and Berg.

Applicant respectfully traverses each of the rejections and submits that none of the cited prior art, taken alone or in combination with other art, discloses or suggests each and every feature of the claims.

Claim 3, upon which claims 27-38 depend, recites a computer system comprising a dual-kernel operating system that includes a real-time kernel and a non-real-time kernel with a first real-time thread executing under the real-time kernel that is ***configured to monitor the integrity of an application*** running under the non-real-time kernel and a second real-time thread running under the real-time kernel is configured to monitor integrity of the first real-time thread, and a security process running under the non-real-time kernel which is configured to check the integrity of the first real-time thread and/or the second real-time thread.

The Examiner cites to REDSonic in combination with Douglas as allegedly rendering these features obvious. REDSonic is alleged to teach a dual-kernel operating

system comprising a real time kernel and a non-real-time kernel, a first real-time thread running under the real-time kernel, the first real-time thread being configured to monitor an application running under the non-real-time kernel. Douglas is cited as teaching the feature of the first thread being configured to monitor the integrity of an application and a second real-time thread running under the real-time kernel.

The combination of REDSonic and Douglas, quite simply, does not teach or suggest all of the features of claim 3. Applicants admit that REDSonic discloses a dual-kernel operating system comprising a real time kernel and a non-real-time kernel, a first real-time thread running under the real-time kernel. As the REDSonic reference notes on page 1, the dual kernel approach was previously disclosed by the creators of RTLinux. In fact, the inventor of the present application is the creator of RTLinux, and this concept is embodied in his U.S. Patent 5,995,745.

The REDSonic reference does not however disclose or teach a first real-time thread being configured to monitor an application running under the non-real-time kernel. The portion of REDSonic cited by the Office Action discloses a layer that is inserted between the interrupt-control hardware and the standard Linux kernel. This layer acts to isolate standard Linux from the interrupt control hardware. As the REDSonic reference notes, this approach allows for the layer executing on the real-time kernel to suspend execution of standard Linux whenever an interrupt arrives. This, however, is not the same as the claimed first real-time thread being configured to monitor an application running under a non-real-time kernel. The layer executing under a real-time thread in REDSonic is monitoring interrupt control hardware and not an application running under

the non-real-time kernel as required by claim 3. Thus, REDSonic fails to disclose or suggest each and every element of claim 3.

The Examiner attempts to remedy some of the deficiencies of REDSonic with Douglas. The Office Action alleges that "Douglas has integrity checking feature which would require real time processing in order to maintain the integrity of applications." However, as discussed above with respect to claims 1 and 2, Douglas does not disclose the use of hard real-time as is disclosed by the present application and the term "real-time" as used in Douglas has a fundamentally different meaning than as used in claim 3. Furthermore, Douglas does not disclose using threads, running under a real-time kernel or non-real-time kernel, to monitor the integrity of other executing threads or an application as required by the claims. Yodaiken Decl. ¶¶ 20-21. Monitoring system and audit logs, as described in Douglas, would not require the use of a hard real-time operating system which would require that tasks be performed within a specified, fixed period of time. The term "real-time" as used in Douglas is clearly referring to a process that monitors a system on an ongoing basis, and not to hard real-time as used in the present application. Thus, Douglas fails to remedy the above-described deficiencies of REDSonic, and neither REDSonic nor Douglas discloses each and every element of claim 3.

Moreover, one of ordinary skill in the art, viewing REDSonic, and Douglas at the time of the invention, would not have arrived at the invention of the present application, without the benefit of the present claims as a roadmap, i.e., without relying on improper hindsight in attempting to combine the references to arrive at the present claims. Thus, for this separate and independent reason, this rejection is improper.

In addition to the foregoing, strong secondary evidence exists that proves that the claims of the present application are nonobvious. Namely, hard real-time operating systems and concepts have existed for a number of years, yet there is no system known to the inventor or cited by the Examiner, prior to the invention described by the present application, which discloses these features. Software security is an area in which a great deal of research and effort has been applied in recent years. Yodaiken Decl. ¶ 32. The fact that no known system applies these hard real-time concepts in the manner of the present claims is a strong indication of the non-obviousness of the claims. Thus, for this additional, separate reason, the rejection to the claims in improper.

Accordingly, the Applicant requests that the rejection to claims 3 and to claims 27-38 which depend thereon be withdrawn.

In view of the foregoing and the declaratory evidence submitted herewith, which should be given substantial weight, Applicants submit that the rejection of each of claims 1-7, 14-20 and 25-44 is improper because the cited prior art fails to disclose or suggest each and every element of the claims, one having ordinary skill in the art would not have been motivated to derive the invention therefrom, and the rejection is based on impermissible hindsight. Accordingly, Applicants request that the rejections be withdrawn and that claims 1-7, 14-20 and 25-44 be allowed.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event that this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account No. 02-2135.

Respectfully submitted,

By _____

Martin M. Zoltick, Reg. No. 35,745
Attorney for Applicant
Rothwell, Figg, Ernst & Manbeck, P.C.
Suite 800, 1425 K Street, NW
Washington, D.C. 20005
Telephone: (202) 783-6040
Facsimile: (202) 783-6031

1492644_1